8 The Pila-Zannier proof of the Manin-Mumford Conjecture

My goal in these lecture notes is to describe a variant of the Pila-Zannier proof of the Manin-Mumford Conjecture.[3]

Theorem 8.1 *Let A be an abelian variety defined over a number field. Suppose $V \subseteq A$ is an irreducible subvariety. There are finitely many cosets of algebraic subgroups $b_1 + B_1, \ldots, b_n + B_n$ such that each $b_i + B \subseteq V$ and $V \cap \mathrm{Tor}(A) \subseteq b_1 + \mathrm{Tor}(B_1) \cup \ldots \cup b_n + \mathrm{Tor}(B_n)$. In particular, if V contains no cosets of infinite algebraic subgroups, then $V \cap \mathrm{Tor}(A)$ is finite.*

The novelty of the Pila-Zanier proof is that it relies on a result of Pila and Wilkie on the asymptotics of rational points on sets definable in o-minimal structures. As such it is the only proof of Manin-Mumford that relies on real– rather than p-adic–methods.

Let $x \in \mathbb{Q}$, $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, we define $h(x)$ the *height* of x to be the maximum of $|a|$ and $|b|$. If $x = (x_1, \ldots, x_n) \in \mathbb{Q}^n$ we let $h(x)$ be the maximum of $h(x_1), \ldots, h(x_n)$.

For $X \subseteq \mathbb{R}^n$ and $r \in \mathbb{R}$ we let $N(X, r)$ be the number of points in $X \cap \mathbb{Q}^n$ of height at most r.

For $X \subseteq \mathbb{R}^n$ we let X^{alg} be the union of all connected infinite semialgebraic subsets of X.

Theorem 8.2 (Pila-Wilkie) *Suppose $X \subseteq \mathbb{R}^n$ is definable in an o-minimal expansion of $\mathbb{R}$. Then for any $\epsilon > 0$ there is a constant c such that*

$$N(X \setminus X^{\mathrm{alg}}, r) < cr^{\epsilon}$$

for all $r \geq 1$.

The case of Tori

As an instructive example we will first prove the theorem where we work with $\mathbb{G}_m^d$, a power of the multiplicative group rather than an Abelian variety.

Step 1 Move to an o-minimal setting.

Let $g : [0, 1]^d \to \mathbb{C}^d$ be defined be the function

$$g(x_1, \ldots, x_d) = (2\pi i x_1, \ldots, 2\pi i x_d)$$

and let $\exp : \mathbb{C}^d \to \mathbb{G}_m^d$ be the function

$$\exp(y_1, \ldots, y_d) = (e^{y_1}, \ldots, e^{y_d}).$$

[3]These lectures are based on notes of Anand Pillay.

Let $f = \exp \circ g$.

If $a \in \mathbb{G}_m$ has order n, then $a = e^{2\pi i \frac{m}{n}}$ where $0 < m < n$ and m and n are relatively prime. Thus $\mathrm{Tor}(\mathbb{G}_m^d)$ is contained in the image of f on $[0,1]^d \cap \mathbb{Q}^d$. Let $X = f^{-1}(V)$.

If we identify $\mathbb{C}^d$ with $\mathbb{R}^{2d}$ in the usual way, then

$$f(x_1, \ldots, x_n) = (\cos(2\pi x_1), \sin(2\pi(x_1), \ldots, \cos(2\pi x_n), \sin(2\pi(x_n)).$$

In particular, then f and X are definable in the o-minimal structure $\mathbb{R}_{\mathrm{an}}$.

Step 2 Understand X^{alg}

If $x \in X^{\mathrm{alg}}$, then there is a connected one-dimensional semialgebraic set C such that $x \in C$. By quantifier elimination it is easy to see the C is a piece of a real algebraic curve.

Our analysis will use Ax's differential field version of Schanuel's Conjecture.

Theorem 8.3 (Ax) *Let (K, δ) be a differential field with constants k. Suppose $y_1, \ldots, y_n, z_1, \ldots z_n \in K$ such that $\delta(y_i) = \frac{\delta(z_i)}{z_i}$ for $i = 1, \ldots, n$. Suppose the transcendence degree of $k(y_1, \ldots, y_n, z_1, \ldots, z_n)$ over k is at most n, then there are integers $m_1, \ldots, m_n$ such that:*

i)

$$\prod_{i=1}^{n} z_i^{m_i} \in k,$$

and

ii)

$$\sum_{i=1}^{n} m_i y_i \in k.$$

If B is an infinite irreducible algebraic subgroup of $\mathbb{G}_m^d$. There is a $k \times d$ integer matrix $M = (a_{i,]})$ such that

$$z \in B \leftrightarrow \prod_{j=1}^{d} z_j^{a_{i,j}} = 1, \text{ for } i = 1, \ldots, k.$$

Define $LB \subseteq \mathbb{C}^d$, $LB = \{y : My = 0\}$.

Suppose $C \subseteq X$ is a connected one-dimensional semialgebraic set and x is a generic point of C, in the sense of the o-minimal structure $\mathbb{R}_{\mathrm{an}}$. As above, let $y = g(x)$ and $z = \exp(y)$.

Lemma 8.4 *Let B be a minimal irreducible algebraic subgroup of $\mathbb{G}_m^d$ such that $y \in b + LB$ for some $b \in \mathbb{C}^d$. Then the transcendence degree of $\mathbb{C}(z)$ over $\mathbb{C}$ is the dimension of B and $\exp(b) + B$ is contained in V.*[4]

[4]To make the transition to the case of Abelian varieties smoother, we abuse notation and write cosets in $\mathbb{G}_m^d$ additively.

Proof Let l be the dimension of LB. Since x is a generic point we must have $l > 0$.We may, without loss of generality, assume that $y_1, \ldots, y_l$ satisfies no equation $\sum m_i y_i = c$ where $m_i \in \mathbb{Z}$ and $c \in \mathbb{C}$. We claim that $z_1, \ldots, z_l$ are algebraically independent over $\mathbb{C}$. Suppose not. Since $x \in C$, $\mathrm{td}(y/\mathbb{C}) = \mathrm{td}(x/\mathbb{C}) = 1$. Then $\mathrm{td}(y_1 \ldots, y_l, z_1, \ldots, z_l/\mathbb{C})$ is at most n. Thus by Ax, there are $m_1, \ldots, m_l$ such that $\sum m_i y_i \in \mathbb{C}$, a contradiction.

Thus z is an (algebraic) generic point of $\exp(b)+B$. Since $z \in V$, $\exp(b)+B \subseteq V$.

Corollary 8.5 *If $a \in X^{\mathrm{alg}} \cap \mathbb{Q}^d$, then $f(a) \in b + B$ where b is a torsion point of A, B is an infinite algebraic subgroup of A and $b + B \subseteq V$.*

Step 3 Finiteness of $\mathbb{Q}^d \cap X \setminus X^{\mathrm{alg}}$

We may, without loss of generality, assume that $V \cap \mathrm{Tor}(\mathbb{G}_m^d)$ is Zariski dense in V. If not, then we can proceed by first proving the result for each irreducible component of the Zariski closure of $V \cap \mathrm{Tor}(\mathbb{G}_m^d)$. Then, any automorphism of $\mathbb{C}$ that fixes the roots of unity will fix V. Thus V is defined over a number field k. We may assume that k is a Galois extension of $\mathbb{Q}$ of degree l.

Suppose $a = (a_1, \ldots, a_d) \in V \cap \mathrm{Tor}(G_m^d)$. If σ is an automorphism of $\mathbb{C}$, fixing k, then $\sigma(a) \in V \cap \mathrm{Tor}(\mathbb{G}_m^d)$.

Let a_1 have order exactly n_i then a has order n where n is the least common multiple of $n_1, \ldots, n_m$. If b is a primitive n^{th}-root of unity, then $\mathbb{Q}(b) = \mathbb{Q}(a_1, \ldots, a_d)$. Thus the degree of $k(a)/k$ is at most $\phi(n)$ and at least $\phi(n)/l$., where $\phi(n)$ is Euler's function, i.e.,

$$\phi(n) = |\{m : 1 \leq x < n, x \text{ relatively prime to } n\}|.$$

The asymptotics of $\phi(n)$ are well understood. In particular, for any $0 < \epsilon < 1$,

$$n^\epsilon < \phi(n)$$

for large enough n.[5] In particular there is M such that if $a \in \mathrm{Tor}(\mathbb{G}_m^d)$ is a torsion point of order $n > M$, then a has at least $\frac{n^{1/2}}{l}$ conjugates over k.

Suppose $a \in V \cap \mathrm{Tor}(\mathbb{G}_m^d)$ is not in an infinite coset $b+B$ where $b+B \subseteq V$. Then the same is true of all conjugates of a over k. If a has order n, there is $x \in (X \setminus X^{\mathrm{alg}}) \cap \mathbb{Q}^d$ such that $f(x) = a$ and $h(x) = n$. Thus if $(X \setminus X^{\mathrm{alg}}) \cap \mathbb{Q}^d$ is infinite, then

$$N(X \setminus X^{\mathrm{alg}}, n) \geq \frac{n^{1/2}}{l}$$

for infinitely many n. But this contradicts the Pila-Wilkie Theorem.

Corollary 8.6 *There is a finite set F such that every element of $V \cap \mathrm{Tor}(\mathbb{G}_m^d)$ is either contained in F or contained in $b + B$ where $b \in \mathrm{Tor}(\mathbb{G}_m^d)$ and B is an infinite irreducible algebraic subgroup of $\mathbb{G}_m^d$.*

[5] Better bounds can be found using the Prime Number Theorem.

We say that an infinite irreducible coset $b + B$ is *maximal* $b + B \subseteq V$ and there is no irreducible algebraic subgroup $C \supset B$ with $b + C \subseteq V$. We need to show there are only finitely many maximal cosets $b + B \subseteq V$.

Step 4 Finitely many choices for B.

Bombieri and Zannier proved, in the Abelian variety case, that there are only finitely many B such that $b+B$ is a maximal coset in V. This follows from the next two lemmas.

Lemma 8.7 *For any M there are only finitely many subgroups of $\mathbb{G}_m^d$ of degree M.*

Proof For any dimension $m < d$, there is a definable family $(W_y : y \in Y)$ of all subvarieties of $\mathbb{G}_m^d$ of dimension m and degree M. There is a definable $Y_0 \subseteq Y$ such that $y \in Y_0$ if and only if W_y is a subgroup. Since semi-abelian varieties have no infinite definable families of subgroups Y_0 is finite.[6]

Lemma 8.8 *There is a number M, depending on the dimension and the degree of V such that if $b + B$ is a maximal coset then the degree of B is at most M.*

Proof Suppose $b + B$ is a maximal coset. We build a sequence of subvarieties $V = V_1 \supset V_2 \supset \ldots \supset V_m$ as follows. Given V_i if there is $g \in B$ such that

$$\dim(V_i \cap V_i + g) < \dim V_i,$$

then choose some such g and let V_{i+1} be an irreducible component of the intersection containing $b + B$. If there is no such $g \in B$, we let $m = i$. Let $W = V_i$. Since $m < \dim V$, we can bound $\deg W$ in terms of the dimension and degree of W.

Note that $b \in W$ and $B + W = W$.

We next build a sequence $W = W_1 \supset W_2 \supset \ldots \supset W_m$ such that $b+B \subseteq W_i$ and $B + W_i = W + i$ for all i. Start with W_i. If there is $x \in W_i$ such that

$$\dim(W_i \cap (b - x) + W_i) < \dim W_i$$

then we choose some such x. Let $Y_1, \ldots, Y_m$ be the irreducible components of $W_i \cap (b - x) + W_i$. Note that $b + B \subseteq (b - x) + W_i$. Thus $b + B$ is contained in one irreducible component, say Y_1. Let $B_0 = \{b \in B : b + Y_1 = Y_1\}$. Then B_0 is a finite index subgroup of B. But B is irreducible, so $B = B_0$ and $B + Y_1 = Y_1$. Let $Y_1 = W_{i+1}$. If there is no such x, we let $m = i$ and stop.

Let $Z = W_m$. Once again, we can bound the degree of Z in terms of the dimension and degree of V. We also have that $Z$is irreducible, $b + B \subseteq Z$, $Z + B = B$ and $b - z + Z = Z$ for all $z \in Z$.

Let $C = \{a \in \mathbb{G}_m^d : a + Z = Z\}$. Then C is an algebraic subgroup of A and $B \subseteq C$. Since $C + Z = Z$ and $b \in Z$, $b + C \subseteq Z \subseteq V$, thus, by the maximality of V, C is a finite union of B cosets.

[6]This is really much easier for $\mathbb{G}_m^d$ where we can easily describe the subgroups.

On the other hand, $B \subseteq b-Z$, while, by construction of Z, $b-Z \subseteq C$. Since Z is irreducible we must have $B = b - Z$. Thus we can bound the degree of B.

We can now finish the proof. We claim that for any infinite irreducible subgroup B, there are only finitely many maximal cosets $b + B \subseteq V$ where b is a torision point of A.

Suppose for contradiction that there are infinitely many maximal torsion cosets $b + B \subseteq V$. Consider the projection map $\pi : A \to A/B$. Let $W = \{a : a + B \subseteq V\}$. Let W' be the projection of W. If V contains infinitely many maximal torsion cosets $b + B$, then W' contains infinitely many torsion points. By the arguments above we can find $b \in W$ such that $b + B$ is a maximal coset and $\pi(b)$ is contained is an infinite torision coset $\pi(b) + C$ of W'. But that $b + \pi^{-1}(C)$ is a coset in V with $\pi^{-1}(C) \supset B$, contradicting the maximality of B.

Abelian Varieties

We outline the changes that need to be made to adapt the argument for Abelian varieties rather than the multiplicative group.

Step 1

We let $\exp_A : \mathbb{C}^d \to A$ be the usual exponential map. Let $\Lambda = \oplus_{i=1}^{2d} \mathbb{Z}\lambda_i$ be the kernel of $\exp_A$. Let $g : [0,1]^{2d} \to \mathbb{C}^d$ be the map

$$g(x_1, \ldots, x_{2n}) = \sum_{i=1}^{n} x_i \lambda_i$$

and let f be the composition $\exp_A \circ g$. Once again, we can view f as a function definable in $\mathbb{R}_{\rm an}$ and $\mathrm{Tor}(A)$ is contained in the image of $[0,1]^{2d} \cap \mathbb{Q}^{2d}$.

Step 2

We need the extension of Ax's theorem for abelian, or semiabelian varieties defined over the constants due independently to Bertrand and Kirby.

Theorem 8.9 (Bertrand/Kirby) *Let K be a differential field with constants k. Suppose A is a semiabelian variety defined over k with Lie algebra LA. Let $l_A : A \to LA$ and $l_{LA} : LA \to LA$ be the logarithmic derivatives. Suppose $(y, z) \in LA \times A$ with $l_{LA} y = l_A z$. If $td(y, z/k) \leq \dim A + 1$, then there is a proper algebraic $B \leq A$ such that:*
i) $z \in B + b$, for some $b \in A(k)$;
ii) $y \in LB + c$, for some $c \in LA(k)$.

Step 3

We need the following Theorem of Masser.

Theorem 8.10 (Masser) *Suppose A is an abelian variety defined over a number field k. There is $l > 0$, $c > 0$ and $N > 0$ such that if a is a torsion point of A of order $n \geq N$, then the degree of a over k is at least $cn^{1/l}$.*

The remainder of the proof is as above.

Semiabelian Varieties

Let's consider the case where G is a semiabelian variety defined over a number field. Suppose $\mathbb{G}_m^d$ is a subgroup of G and the projection map $\pi : G \to A$ has kernel $\mathbb{G}_m^d$ and A is an abelian variety. We suppose that G, A and π are all defined over a number field k.

The n-torsion subgroup of G is of the form $B \oplus C$ where B is the n-torsion of A and π maps C isomorphically onto the n-torsion of A. If $g \in G$ has order n, then $g = b + c$ where $b \in B$ has order n_1, $c \in C$ has order n_2 and n is the least common multiple of n_1 and n_2. At least one of n_1 and n_2 is at least $\sqrt{n}$. Suppose $n_2 \geq \sqrt{n}$. For n large enough and c and l as in Theorem 8.10, $\pi(c)$ has at least $cn^{\frac{1}{2l}}$ conjugates over k. then the same is true of c and g. The argument is similar if $n_1 \geq \sqrt{n}$.

Questions

• Raynaud showed, using specialization arguments, that one could deduce the general version of Manin-Mumbford, from the number field version. Masser's Theorem is the one place we used the number field assumption. Are there extensions of Masser's Theorem that would allow us to deduce the general result by these methods?